Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Combinatorial Theory, Series A 113 (2006) 779–798

Journal of Combinatorial Theory Series A

www.elsevier.com/locate/jcta

Construction of bent functions via Niho power functions

Hans Dobbertin[a], Gregor Leander[a,*], Anne Canteaut[b], Claude Carlet[b], Patrick Felke[a], Philippe Gaborit[c]

[a] *Ruhr-University Bochum, Postfach 102148, 44780 Bochum, Germany*
[b] *INRIA-Projet CODES, BP 105, 78153 Le Chesnay Cedex, France*
[c] *Equipe Arithmtique Codage et Cryptographie, Universite de Limoges, France*

Received 22 November 2004
Available online 26 September 2005

Abstract

A Boolean function with an even number $n = 2k$ of variables is called bent if it is maximally nonlinear. We present here a new construction of bent functions. Boolean functions of the form $f(x) = \mathrm{tr}(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$, $\alpha_1, \alpha_2, x \in \mathrm{F}_{2^n}$, are considered, where the exponents d_i $(i = 1, 2)$ are of Niho type, i.e. the restriction of x^{d_i} on F_{2^k} is linear. We prove for several pairs of (d_1, d_2) that f is a bent function, when α_1 and α_2 fulfill certain conditions. To derive these results we develop a new method to prove that certain rational mappings on F_{2^n} are bijective.

Keywords: Boolean function; Bent function; Niho exponent

1. Introduction

Bent functions are maximally nonlinear Boolean functions with an even number of variables. They were introduced by Rothaus [11] in 1976. Because of their own sake as interesting combinatorial objects, but also because of their relations to coding theory (Reed–Muller codes) and applications in cryptography (design of stream ciphers), they have attracted a lot of research, specially in the last 10 years.

* Corresponding author.
E-mail address: gregor.leander@rub.de (G. Leander).

0097-3165/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2005.07.009

A complete classification of bent functions is elusive and looks hopeless. On the other hand, many special explicit constructions are known, primary ones giving bent functions from scratch and secondary ones building a new bent function from one or several given bent functions. All known primary constructions of bent functions, with only one recent exception (see [1,3]), are weakly normal (cf. [4]). Here a Boolean function with n variables, n even, is called weakly normal (resp., normal) if it is affine (resp., constant) on some affine subspace of dimension $n/2$.

In the present paper, we study traces of a linear combination of two Niho power functions. A power function on F_{2^n} is called a Niho power function if its restriction to $\mathrm{F}_{2^{n/2}}$ is linear. This implies weak normality. In this way, under certain conditions, we get as our main results (Theorems 1–3) three primary construction of bent functions. The starting point of our proofs confirming the bent property is based on a classical theorem of Niho [9] and new methods to handle Walsh transforms of Niho power functions from [7].

2. Preliminaries

Throughout this paper let $L = \mathrm{F}_{2^n}$ be a finite field of characteristic 2, where $n = 2k$, and let $K = \mathrm{F}_{2^k}$ the subfield of L with $[L : K] = 2$. Like every quadratic field extension, the field extension L/K has strong similarities with the extension $\mathbb{C}$, the field of complex numbers, over the field of real numbers $\mathbb{R}$. The *conjugate* of $x \in L$ over K will be denoted by $\overline{x}$, i.e.

$$\overline{x} = x^{2^k}.$$

We denote the *absolute trace* on L by

$$\mathrm{tr}_L(x) = \sum_{i=0}^{n-1} x^{2^i}, \quad x \in L$$

and

$$\mathrm{tr}_{L/K}(x) = x + \overline{x}$$

refers to the relative trace from L onto K. Note that according to the transitivity law for the trace function, we have

$$\mathrm{tr}_L = \mathrm{tr}_K \circ \mathrm{tr}_{L/K}.$$

The relative norm with respect to L/K is defined as

$$\mathrm{norm}_{L/K}(x) = x\,\overline{x}$$

and maps L onto K. The canonical additive character on L is defined as

$$\chi_L(x) = (-1)^{\mathrm{tr}_L(x)}.$$

The *unit circle* of L is the set

$$\mathcal{S} = \{u \in L : u\overline{u} = 1\}$$

of all elements having relative norm 1. In other words, $\mathcal{S}$ is the group of (2^k+1)st roots of unity, and therefore the order of S is 2^k+1, since L^* is cyclic and 2^k+1 divides 2^n-1.

Note that $\mathcal{S} \cap K = \{1\}$ and each non-zero element of L has a unique *polar coordinate representation*, i.e.

$$x = \lambda u$$

with $\lambda \in K^*$ and $u \in \mathcal{S}$. According to the analogy to $\mathbb{C}/\mathbb{R}$ we write $\lambda = \|x\|$ for the *length* and $u = \varrho(x)$ for the *angle* of x. We have [1]

$$\|x\| = \sqrt{x\overline{x}}, \tag{1}$$

$$\varrho(x) = \sqrt{x/\overline{x}}. \tag{2}$$

2.1. Walsh transforms and bent functions

For a moment we do not require that n is even. We identify the Galois field $L = \mathrm{F}_{2^n}$ with F_2^n by choosing a base of L, considered as vector space over F_2. The notion of a Walsh transform refers to a scalar product. Thus, it is convenient to choose the basis, such that the canonical scalar product $\langle \cdot, \cdot \rangle$ in F_2^n coincides with the scalar product in L, which is the trace of the product

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i = \mathrm{tr}_L(xy), \quad x, y \in L.$$

A *Boolean function* f is a mapping from L into F_2. The *Walsh transform* of f is defined as

$$f^{\mathcal{W}}(c) = \sum_{x \in L} (-1)^{f(x)} \chi_L(cx), \quad c \in L.$$

The maximal absolute values attained by $f^{\mathcal{W}}$ is a measure for the *linearity* of f

$$\mathrm{Lin}\, f = \max_{c \in L} |f^{\mathcal{W}}(c)|.$$

Obviously we have the upper bound

$$2^n \geqq \mathrm{Lin}\, f$$

and it is attained if and only if f is affine. On the other hand, as a consequence of *Parseval's equation*

$$\sum_{c \in L} f^{\mathcal{W}}(c)^2 = 2^{2n}, \tag{3}$$

[1] The symbol $\sqrt{X}$ stands for the inverse of the Frobenius mapping $\varphi(X) = X^2$, which makes sense, as we deal with *finite* fields of characteristic 2. Concretely here $\sqrt{z} = z^{2^{k-1}}$ for $z \in K = \mathrm{F}_{2^k}$.

we have

$$2^{n/2} \leqq \mathrm{Lin}\, f.$$

This lower bound is tight if and only if $n = 2k$ is even. By definition f is *bent* if $\mathrm{Lin}\, f = 2^k$ and in this case the Walsh spectrum consist precisely of the values $\pm 2^k$. The simplest example of a bent function is

$$f(x) = \mathrm{tr}_K(\|x\|).$$

The *dual* f^* of a bent function f is defined by the signs attained in the Walsh transform of f

$$f^{\mathcal{W}}(c) = (-1)^{f^*} 2^k.$$

The dual of a bent function is again a bent function, and we have the rule $f^{**} = f$.

2.2. Niho power functions

We say that d (always understood modulo $2^n - 1$) is a *Niho exponent* and x^d is a *Niho power function*, if the restriction of x^d to F_{2^k} is linear or in other words

$$d \equiv 2^i \pmod{2^k - 1}$$

for some $i < n$. Without loss of generality we can assume that d is in the *normalized form* with $i = 0$, and then we have a unique representation

$$d = (2^k - 1)s + 1$$

with $2 \leqq s \leqq 2^k$, because here s and s' give the same power function d on F_{2^n} iff $s \equiv s' \pmod{2^k + 1}$.

The conjugated exponent corresponding to a normalized $d = (2^k - 1)s + 1$, i.e. $d' = 2^k d$, is of the same type, where s has to be replaced by $1 - s \pmod{2^k + 1}$:

$$2^k d = (2^k - 1)(1 - s) + 1 \pmod{2^n - 1}.$$

From this point of view we see that there are two equivalent ways to normalize a Niho exponent. The sum of the corresponding two values for s equals 1 (modulo $2^k + 1$).

The inverse of a Niho exponent, if it exists, is again of Niho type: in fact, for $d = (2^k - 1)s + 1$ we have $\gcd(d, 2^n - 1) = 1$ if and only if $2s - 1$ is invertible modulo $2^k + 1$, i.e. $\gcd(2s - 1, 2^k + 1) = 1$, and in this case

$$d^{-1} = (2^k - 1)s' + 1 \pmod{2^n - 1}, \quad s' = s/(2s - 1) \pmod{2^k + 1},$$

since $d((2^k - 1)s' + 1) = -2(-2ss' + s + s') + 1 = 1 \pmod{2^k + 1}$.

2.3. Convention

If some s, used to define a Niho exponent as above, is written as a fraction, then this has to be interpreted modulo $2^k + 1$. For instance

$$s = \tfrac{1}{2} = 2^{k-1} + 1.$$

3. Main results

Let $L = \mathrm{F}_{2^n}$ and $n = 2k$. We consider Boolean functions

$$f(x) = \mathrm{tr}_L(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$$

on L, for $\alpha_1, \alpha_2 \in L$, where the $d_i = (2^k - 1)s_i + 1$, $i = 1, 2$, are Niho exponents. We conjecture that if f is bent, then necessarily w.l.o.g.

$$d_1 = (2^k - 1)\,\tfrac{1}{2} + 1.$$

This conjecture is suggested by computer experiments. In the sequel we require this choice of d_1. Recall that here $s_1 = \frac{1}{2}$ has to be understood modulo $2^k + 1$, that is $\frac{1}{2} = 2^{k-1} + 1$. Observe that d_1 is cyclotomic equivalent to $2d_1 = 2^k + 1$ and we have

$$x^{d_1} = \sqrt{x\overline{x}} = \|x\|.$$

This special choice of d_1 implies that replacing α_1 by α_1' does not change f if (and only if) $\alpha_1 + \alpha_1' \in K$.

For $\alpha_2 = 0$, we obtain bent functions iff $\alpha_1 \notin K$

$$f(x) = \mathrm{tr}_L(\alpha_1 x^{d_1}) = \mathrm{tr}_L(\alpha_1 \|x\|) = \mathrm{tr}_K((\alpha_1 + \overline{\alpha_1})\,\|x\|),$$

which belong to a trivial class of bent function, the quadratic ones. It seems that there are no more bent functions of the form $f(x) = \mathrm{tr}_L(\alpha x^d)$ with Niho exponent d.

For the following theorems we require that:

$$\alpha_1 + \overline{\alpha_1} = \|\alpha_2\|.$$

However, this general form can easily be reduced to the case $\alpha_2 = 1$, as we shall see.

Theorem 1. *Define*

$$d_2 = (2^k - 1)\,3 + 1.$$

If $k \equiv 2 \pmod 4$ *assume that* $\alpha_2 = \beta^5$ *for some* $\beta \in L^*$. *Otherwise, i.e. if* $k \not\equiv 2 \pmod 4$, $\alpha_2 \in L^*$ *is arbitrary. Then f is a bent function with degree*[2] k.

From $\omega(d_2) = \omega(2^k + (2^{k-1} - 1)) = 1 + (k-1) = k$ we conclude that f, as a multi-variate binary function, has in fact degree k, the maximal degree a bent functions can attain.

Theorem 2. *Suppose that k is odd. Define*

$$d_2 = (2^k - 1)\,\tfrac{1}{4} + 1.$$

Then f is a bent function of degree 3.

[2] We identify $L = \mathrm{F}_{2^n}$ with F_2^n. The binary degree of the n-variate polynomials representing a function of the form $\mathrm{tr}(\alpha x^d)$, which is not identically zero, is precisely the Hamming weight $\omega(d)$ of the binary representation of d (reduced modulo $2^n - 1$).

Observe that d_2 is cyclotomic equivalent to and can be replaced by

$$4d_2 = 2^k + 3.$$

From $\omega(4d_2) = 3$ we conclude that f has degree 3.

Theorem 3. *Suppose that k is even. Define*

$$d_2 = (2^k - 1)\,\tfrac{1}{6} + 1.$$

Then f is a bent function of degree $k/2 + 1$.

Note that

$$2d_2 = (1 + 4 + 16 + \cdots + 2^{k-2}) + 2$$

and therefore $\omega(d_2) = k/2 + 1$ and consequently f has indeed degree $k/2 + 1$.

Remark 4. The preceding theorems were conjectured based on computer experiments carried out by Canteaut, Carlet and Gaborit for $k \leqq 6$. Every example found by that exhaustive search is now covered by one of our theorems. Their proofs in this paper will combine Niho's basic result [9] of 1972 with parts of a recent approach to handle Walsh transforms of Niho power functions, due to Dobbertin et al. [7], (see next section) and new results on certain rational functions inducing one-to-one mappings (see Section 5).

Remark 5. The s_2 in Theorems 1–3 can be replaced by $1 - s_2$, resp., since this does not change the cyclotomic class. Thus, the alternative values are

$$s_2 = -2,\ \tfrac{3}{4},\ \tfrac{5}{6} \pmod{2^k + 1},$$

respectively.

Remark 6. The bent functions given by the preceding theorems for the essential case $\alpha_2 = 1$ do not depend on α_1 and can be written as

$$f(x) = \mathrm{tr}_K(\|x\|) + \mathrm{tr}_L(x^{d_2}) \tag{4}$$

for the respective d_2.

Remark 7. In general, given a bent function of the form

$$f(x) = \mathrm{tr}_L\left(\sum_{i=1}^{m} \alpha_i x^{d_i}\right)$$

for Niho exponents $d_i = (2^k - 1)s_i + 1\,(i = 1, \ldots, m)$, and setting $f_\lambda(x) = f(\lambda x)$ for $\lambda \in K$ we get a collection of bent functions, for $\lambda \neq 0$, such that

$$f_\lambda + f_\mu = f_{\lambda+\mu}$$

for all $\lambda, \mu \in K$. Thus defining

$$C = \{f_\lambda : \lambda \in K\},$$

we obtain a k-dimensional subcode C of the Reed–Muller code $\mathrm{RM}(r, n)$ of order $r = \deg f$, which consists of bent functions and the zero function.

We can put the latter observation into other terms, using the notion of a vectorial bent function. Define $F : L \to K$ as

$$F(x) = \mathrm{tr}_{L/K}\left(\sum_{i=1}^{m} \alpha_i x^{d_i}\right).$$

If $f(x) = \mathrm{tr}_L\left(\sum_{i=1}^{m} \alpha_i x^{d_i}\right)$ is bent then all component functions, i.e. functions of the form $\mathrm{tr}_K(\lambda F(x))$, $\lambda \in K^*$, are bent. In fact

$$\begin{aligned}
\mathrm{tr}_K(\lambda F(x)) &= \mathrm{tr}_K\left(\lambda \mathrm{tr}_{L/K}\left(\sum_{i=1}^{m} \alpha_i x^{d_i}\right)\right) \\
&= \mathrm{tr}_K\left(\mathrm{tr}_{L/K}\left(\lambda \sum_{i=1}^{m} \alpha_i x^{d_i}\right)\right) \\
&= \mathrm{tr}_L\left(\sum_{i=1}^{m} \alpha_i (\lambda x)^{d_i}\right) \\
&= f(\lambda x).
\end{aligned}$$

Kaisa Nyberg [10] refers to the property that all component functions of a vectorial Boolean function are bent by calling them *vectorial bent functions.*

Thus, for the bent functions f in (4) above one obtains, as another way to state our main results:

Theorem 8. *Let $d = (2^k - 1)s + 1$ be a Niho exponent. Then the vectorial Boolean function*

$$F(x) = \|x\| + x^d + \overline{x}^d$$

from L onto K is bent for $s = 3$, for $s = \frac{1}{4}$ if k is odd and for $s = \frac{1}{6}$ if k is even, respectively.

Using Dickson polynomials (see p. 12) and the angle functions ϱ (see (2)) we can represent F for Theorem 8 also in the form

$$F(x) = \|x\|\,(1 + D_{2s-1}(\varrho(x))).$$

A vectorial bent function from F_2^n to F_2^m exists only if $m \leqq k = n/2$ as shown by Kaisa Nyberg [10]. Hence, the dimension of the image vector space of the F in Theorem 8 is maximal.

We recall the previously known constructions of vectorial bent functions. They are straightforward generalizations of classical constructions of bent functions due to Maiorana–McFarland [8] and Dillon [2], respectively. A vectorial bent function $F : K \times K \to K$ is defined by setting

$$F(y, z) = y\,\pi(z) + h(z) \quad (\textit{Maiorana–McFarland construction}),$$

where π is a permutation of K and $h : K \to K$ is any mapping, and by setting

$$F(y, z) = \sigma(y/z) \quad \text{(Dillon construction)}$$

with the convention $y/0 = 0$, where σ is a permutation of K with $\sigma(0) = 0$.

Remark 9. Whenever a new construction of bent functions is found, the question arises, what is the structure of the corresponding dual bent functions. (For instance the constructions of Maiorana–McFarland and Dillon are closed under forming duals.) We presently do not have an answer here.

4. Niho's theorem and Dickson polynomials

Niho's theorem [9] is presented below. For the reader's convenience, we include a proof (cf. [5]).

Theorem 10. *Assume that*

$$d = (2^k - 1)s + 1$$

is a Niho exponent and

$$f(x) = \mathrm{tr}(x^d).$$

Then $f^{\mathcal{W}}(c) = (N(c) - 1)2^k$, where $N(c)$ is the number of $u \in \mathcal{S}$, such that

$$u^{2s-1} + \overline{u}^{2s-1} + cu + \overline{cu} = 0 \tag{5}$$

for each $c \in L = \mathrm{F}_{2^n}$.

Thus the Walsh spectrum of f is at most $2s$-valued, and the occurring values are among

$$-2^k,\ 0,\ 2^k,\ 2 \cdot 2^k, \ldots, (2s-2)\,2^k.$$

Proof. Using the polar coordinate representation and $\mathrm{tr}_L = \mathrm{tr}_K \circ \mathrm{tr}_{L/K}$, we have

$$\begin{aligned}
f^{\mathcal{W}}(c) &= \sum_{z \in \mathrm{F}_{2^n}} \chi_L(cz + z^d) \\
&= 1 + \sum_{u \in \mathcal{S}} \sum_{\lambda \in \mathrm{F}_{2^k}{}^*} \chi_L(c\lambda u + \lambda^d u^d) \\
&= 1 + \sum_{u \in \mathcal{S}} \sum_{\lambda \in \mathrm{F}_{2^k}{}^*} \chi_L(\lambda(cu + u^d)) \\
&= 1 - \#\mathcal{S} + \sum_{u \in \mathcal{S}} \sum_{\lambda \in \mathrm{F}_{2^k}} \chi_K(\lambda(cu + u^d + \overline{c}u^{-1} + u^{-d})) \\
&= -2^k + \sum_{u \in \mathcal{S}} \sum_{\lambda \in \mathrm{F}_{2^k}} \chi_K(\lambda(cu + u^{1-2s} + \overline{c}u^{-1} + u^{2s-1})) \\
&= (N(c) - 1)2^k. \qquad \square
\end{aligned}$$

The same proof shows that more generally if

$$f(x) = \mathrm{tr}_L\left(\sum_{i=1}^{m} \alpha_i x^{d_i}\right)$$

for Niho exponents $d_i = (2^k-1)s_i+1$ $(i = 1, \ldots, m)$, then $N(c)$ is the number of solutions u in $\mathcal{S}$ of

$$cu + \overline{cu} + \sum_{i=1}^{m} \alpha_i u^{1-2s_i} + \sum_{i=1}^{m} \overline{\alpha_i}\, \overline{u}^{1-2s_i} = 0$$

or equivalently by replacing u by $\overline{u}$

$$cu + \overline{cu} + \sum_{i=1}^{m} \alpha_i u^{2s_i-1} + \sum_{i=1}^{m} \overline{\alpha_i}\, \overline{u}^{2s_i-1} = 0.$$

This means for the values of f in Theorems 1–3, where $s_1 = \frac{1}{2}$, that the equation

$$cu + \overline{cu} + \alpha_1 + \overline{\alpha_1} + \alpha_2 u^{2s_2-1} + \overline{\alpha_2}\, \overline{u}^{2s_2-1} = 0 \tag{6}$$

has to be considered. We assume that $\alpha_1 + \overline{\alpha_1} = \alpha_2 = 1$. (The assertion of our theorems can easily be reduced to that case, see Section 6.) Therefore in order to confirm that f is bent, setting $s = s_2$ we have to show that the number of roots u in $\mathcal{S}$ of

$$G_c(u) = u^{2s-1} + \overline{u}^{2s-1} + cu + \overline{cu} + 1 = 0 \tag{7}$$

is either 0 or 2.

Remark 11. Niho's theorem in combination with Parseval's equation (3) obviously implies that it suffices to prove that (7) has at most 2 solutions. But we do not use this argument, since it does not simply our proofs essentially.

In [7], the value distribution of the Walsh spectrum of $\mathrm{tr}(x^{d_2})$ for $d_2 = (2^k - 1)\,3 + 1$ of Theorem 1 has been determined for odd k. This requires to analyze the number of solutions of the following closely related equation for $s = 3$:

$$u^5 + \overline{u}^5 + cu + \overline{cu} = 0.$$

This problem was settled with the development of a new approach using Dickson polynomials [7], which will be explained below. It is also the basic tool for proving the results of the present paper.

Given $c \in L \setminus K$ the idea of Dobbertin et al. [7] is to consider c, $\overline{c}$ and the associated equations $G_c(u) = 0$ and $G_{\overline{c}}(u) = 0$ simultaneously:

$$G_c(u)\, G_{\overline{c}}(u) = 0. \tag{8}$$

Then we can change from the parameters $u \in \mathcal{S}$ and $c \in L$ to new parameters β, resp., γ, T and N in the small field K. The advantage of this procedure is that we end up with an

equation, where we have to count the solutions with a special "trace condition" instead of counting solutions with a "norm condition", which turns out to be much easier.

The twins $c, \overline{c} \in L \setminus K$ are replaced by the coefficients of their (common) minimal polynomial

$$m_{c,\overline{c}} = X^2 + TX + N$$

over K, that is

$$T = \mathrm{tr}_{L/K}(c) = \mathrm{tr}_{L/K}(\overline{c}) = c + \overline{c},$$
$$N = \mathrm{norm}_{L/K}(c) = \mathrm{norm}_{L/K}(\overline{c}) = c\,\overline{c}.$$

Necessary and sufficient conditions for $T, N \in K$ to represent $c, \overline{c} \in L \setminus K$ in this way are $T \neq 0$ and

$$\mathrm{tr}_K(N/T^2) = 1. \tag{9}$$

We recall the following simple, but very important observation:

Fact (*Hilbert 90*). *We have* $\mathrm{tr}_K(x) = 0$ *for* $x \in K$ *if and only if there exists some* $y \in K$ *with* $x = y^2 + y$.

Thus (9) means that $X^2 + TX + N$ is irreducible over K. Fortunately (9) can be ignored in this context, as it is included in (10) below.

Similarly β represents the pair $\{u, \overline{u}\}$ for $u \in \mathcal{S} \setminus \{1\}$ in the sense that

$$m_{u,\overline{u}}(X) = X^2 + \frac{1}{\beta}X + 1$$

or equivalently

$$\beta = \frac{1}{u + \overline{u}}.$$

A necessary and sufficient condition for β to play this role is

$$\mathrm{tr}_K(\beta) = 1.$$

Sometimes it is convenient to make also use of the parameter γ:

$$\gamma = 1/\beta.$$

Changing to the new parameters, $G_c(u)\, G_{\overline{c}}(u)$ can be transformed as follows, where $D_i(X)$ denotes the ith Dickson polynomial over F_2:

$$\begin{aligned} G_c(u)\, G_{\overline{c}}(u) &= \left(u^{2^{s-1}} + \overline{u}^{2^{s-1}} + cu + \overline{cu} + 1\right)\left(u^{2^{s-1}} + \overline{u}^{2^{s-1}} + \overline{c}u + c\overline{u} + 1\right) \\ &= \left(u^{2^{s-1}} + \overline{u}^{2^{s-1}} + 1\right)^2 + \left(u^{2^{s-1}} + \overline{u}^{2^{s-1}} + 1\right)(c + \overline{c})\,(u + \overline{u}) \\ &\quad + (cu + \overline{cu})\,(\overline{c}u + c\overline{u}) \\ &= (D_{2^{s-1}}(\gamma) + 1)^2 + (D_{2^{s-1}}(\gamma) + 1)\,\gamma T + T^2 + \gamma^2 N. \end{aligned}$$

Dickson polynomials satisfy the functional equation

$$D_i(X + X^{-1}) = X^i + X^{-i},$$

the iteration rule

$$D_i(D_j(X)) = D_{ij}(X)$$

and can be obtained by the recursion

$$D_{i+2}(X) = X D_{i+1}(X) + D_i(X)$$

with $D_0(X) = 0$ and $D(X) = X$. We give a list of the Dickson polynomials for $i < 10$

$$\begin{aligned}
&D_0(X) = 0,\\
&D_1(X) = X,\\
&D_2(X) = X^2,\\
&D_3(X) = X^3 + X,\\
&D_4(X) = X^4,\\
&D_5(X) = X^5 + X^3 + X,\\
&D_6(X) = X^6 + X^2,\\
&D_7(X) = X^7 + X^5 + X,\\
&D_8(X) = X^8,\\
&D_9(X) = X^9 + X^7 + X^5 + X.
\end{aligned}$$

Summarizing we have seen that $G_c(u)\, G_{\overline{c}}(u) = 0$ with $u \in \mathcal{S}$ is equivalent to the following equation in K:

$$\left(\frac{(D_{2s-1}(1/\beta) + 1)\beta}{T}\right)^2 + \frac{(D_{2s-1}(1/\beta) + 1)\beta}{T} + \beta^2 = \frac{N}{T^2}. \tag{10}$$

Given T and N we have to count the number of solutions β with trace 1 of (10). Given any non-zero T and β with trace 1, we can interpret (10) as definition of N. This makes sense, because it then follows, as already mentioned above, that $\mathrm{tr}_K(N/T^2) = \mathrm{tr}_K(\beta) = 1$ and therefore T, N represent c, $\overline{c}$ via $m_{c,\overline{c}}(X) = X^2 + TX + N$. We then have to look at the number of solutions of (10) different from the given β (for more details see [7]). The special cases $T = 0$ and 1 have to be considered separately.

5. One-to-one rational functions

After these preparations, the verification of our main results will come down to the following two lemmas (to be honest, they have been found for that reason), as we shall see in the next sections.

Remark 12. The technique used here to prove the below Lemmas 13 and 14 is due to Dobbertin and Leander. It is in some sense similar to the multi-variate method (see [6],

where the multi-variate method is described in its general form), insofar as a "generic" point of view is taken. As for the multi-variate method, also here algebraic computations are applied, which often need Computer Algebra support. Decomposition of multi-variate polynomials (with variables which are considered to be independent) and formal elimination of variables, i.e. for instance computation of resultants, as basic steps.

We briefly describe the method and roughly explain why it works. Suppose that an irreducible multi-variate polynomial $F(a, x_1, \ldots, x_m)$ is given, and that we have to show that $F(a, x_1, \ldots, x_m) = 0$ implies that a has trace 0, i.e. we can represent $a = b^2 + b$ in each of the considered fields. If this fact has "generic" reasons then we can represent these "local" b in a "global" way as a *fixed* rational function of $a, x_1, \ldots, x_m$:

$$b = R(a, x_1, \ldots, x_m) = \frac{C(a, x_1, \ldots, x_m)}{D(a, x_1, \ldots, x_m)}.$$

Assume that R in fact exists. Then $X = b$ is a zero of the rational function

$$(X + R(X^2 + X, x_1, \ldots, x_m))(X + 1 + R(X^2 + X, x_1, \ldots, x_m)).$$

In the generic case we can expect that this rational function is essentially, up to avoiding denominators, the polynomial

$$F(X^2 + X, x_1, \ldots, x_m),$$

which therefore factorizes in the form

$$Q(X, x_1, \ldots, x_m)\, Q(X + 1, x_1, \ldots, x_m).$$

Thus, we consider b as unknown, substitute $a = b^2 + b$ in F and decompose F in order to compute Q. We can assume that a occurs in Q with some odd exponent. Using then $b^2 = b + a$ we reduce Q and get the polynomial $C(a, x_1, \ldots, x_m) + D(a, x_1, \ldots, x_m)b$, which gives $R = C/D$. Common zeros of C and D need an extra discussion.

Given a concrete field K of characteristic 2, we find $b \in E$ with $a = b^2 + b$ in some extension field E of K. Thus, if $F(a, x_1, \ldots, x_m) = 0$ for $a, x_1, \ldots, x_m \in K$, then our generic result implies that $b = R(a, x_1, \ldots, x_m)$ and therefore $b \in K$, i.e. $\mathrm{tr}_K(a) = 0$.

This simple machinery, which works of course for any non-zero characteristic, will turn out to be very powerful and effective.

Define

$$\mathcal{T}_\varepsilon = \{x \in K : \mathrm{tr}_K(x) = \varepsilon\}, \quad \varepsilon \in \mathrm{F}_2.$$

Lemma 13. *Let K be any finite field of characteristic 2. Then the rational functions*

$$\Phi(x) = \frac{1}{x^4} + \frac{1}{x^2} + x$$

and

$$\Psi(x) = \frac{1}{x^8} + \frac{1}{x^2} + x,$$

respectively, induce a permutation of $\mathcal{T}_1$.

Proof. The proof is essentially the same for both rational functions. We consider first $\Phi(x) = 1/x^4 + 1/x^2 + x$. Note that

$$\begin{aligned}\mathrm{tr}(\Phi(x)) &= \mathrm{tr}(1/x^4) + \mathrm{tr}(1/x^2) + \mathrm{tr}(x)\\ &= \mathrm{tr}(1/x) + \mathrm{tr}(1/x) + \mathrm{tr}(x)\\ &= \mathrm{tr}(x).\end{aligned}$$

Thus Φ maps $\mathcal{T}_\varepsilon$ into itself. It remains to confirm that for $\Delta \neq 0$

$$\Phi(x + \Delta) = \Phi(x)$$

implies $\mathrm{tr}(x) = 0$. We have $\Phi(x) = U(x)/V(x)$ with polynomials $U(x) = x^5 + x^2 + 1$ and $V(x) = x^4$. Substituting $x^2 = y^2 + y$ the idea is to represent y as a rational function of x and Δ as described above.[3] We see that the polynomial

$$(\Phi(x + \Delta) + \Phi(x))\, V(x + \Delta)V(x) = U(x + \Delta)V(x) + U(x)V(x + \Delta)$$

factorizes in the form

$$\Delta\, Q(\Delta, y)\, Q(\Delta, y + 1)$$

with

$$Q(\Delta, y) = y^4 + y^3 + \Delta^2 y^2 + \Delta y + \Delta^2.$$

On the other hand, we can write Q uniquely as

$$Q(\Delta, y) = C(\Delta, x^2) + D(\Delta, x^2)y$$

with polynomials C and D. In fact to compute C and D, reduce Q modulo $y^2 = y + x^2$. Here, we have

$$\begin{aligned}C(\Delta, x) &= x^2 + \Delta^2(x + 1),\\ D(\Delta, x) &= x + \Delta^2 + \Delta.\end{aligned}$$

Summarizing we conclude for $\Delta \neq 0$ that $\Phi(x + \Delta) = \Phi(x)$ implies $Q(\Delta, y) = 0$ w.l.o.g., thus $x^2 = y^2 + y$ for $y = C(\Delta, x^2)/D(\Delta, x^2)$. Hence $y \in K$ and $\mathrm{tr}(x) = 0$. It remains to confirm that $C(\Delta, x)$ and $D(\Delta, x)$ have no common zeros x in $\mathcal{T}_1$, which is trivial in our case, since already $D(\Delta, x) = 0$ implies $\mathrm{tr}(x) = 0$.

The other rational function $\Psi(x) = 1/x^8 + 1/x^2 + x$ can get handled in precisely the same way. Here $U(x) = x^9 + x^6 + 1$ and $V(x) = x^8$. This leads to

$$\begin{aligned}Q(\Delta, y) &= y^8 + \Delta y^5 + (\Delta^4 + \Delta^2 + 1)y^4\\ &\quad + (\Delta^3 + \Delta^2 + \Delta)y^3 + \Delta^3 y^2 + \Delta^3 y + \Delta^4\\ C(\Delta, x) &= x^4 + (\Delta^4 + \Delta^2)x^2 + \Delta^4 x + \Delta^4,\\ D(\Delta, x) &= \Delta(x^2 + (\Delta^2 + \Delta)x + \Delta^3 + \Delta^2).\end{aligned}$$

[3] We take $x^2 = y^2 + y$ instead of $x = y^2 + y$, since here $U(x + \Delta)V(x) + U(x)V(x + \Delta)$ is a polynomial in x^2.

$C(\Delta, x)$ and $D(\Delta, x)$ have a common zero Δ if and only if the resultant $\mathrm{res}(C, D, \Delta)$ of C and D with respect to Δ is zero. In this case, we have

$$\mathrm{res}(C, D, \Delta) = x^{14},$$

which is non-zero. In general it suffices here to get a contradiction by showing that the zeros of resultant have trace 0. □

Lemma 14. *Let K be any finite field of characteristic 2 and suppose that $a \in K$ has absolute trace 1. Then the rational functions*

$$R_a(x) = \frac{(x+1)(ax^4 + x^3 + ax^2 + x + a^2)(ax^4 + x^3 + (a+1)x^2 + a^2)}{x(x^4 + x^2 + a)^2 a^2}$$

and

$$S_a(x) = \frac{1}{x} + \frac{x^2 + x}{a(a + x^4 + x^2)},$$

respectively, induce a permutation of $K \setminus \mathrm{F}_2$.

Proof. We first consider R_a. Let $U_a(x)$ and $V_a(x)$ denote the numerator and denominator polynomial of $R_a(x)$, respectively. $V_a(x)$ is non-zero for non-zero x, since $\mathrm{tr}(a) = 1$. We note that $R_a(x)$ can be written as

$$R_a(x) = \frac{\Phi(\sqrt{a} + x^2 + x) + \Phi(\sqrt{a})}{x^2} \tag{11}$$

with Φ (see Lemma 13) defined as

$$\Phi(x) = \frac{1}{x^4} + \frac{1}{x^2} + x.$$

Thus $R_a(x)$ is non-zero for $x \notin \mathrm{F}_2$, since Φ is one-to-one on $\mathcal{T}_1$ by Lemma 13 and a, $a + x^2 + x \in \mathcal{T}_1$.

To confirm that R_a is one-to-one, we argue as before. Suppose on the contrary that $R_a(x) = R_a(y)$ for $x, y \notin \mathrm{F}_2$, $x \neq y$. We have to present $a = b^2 + b$ in K to get a contradiction to $\mathrm{tr}_K(a) = 1$. Substituting $a = b^2 + b$, the polynomial

$$(R_a(x) + R_a(y))\, V_a(x) V_a(y) = U_a(x) V_a(y) + U_a(y) V_a(x)$$

factorizes in the form

$$a^2\,(x + y)\, Q(b, x, y)\, Q(b + 1, x, y)$$

with

$$\begin{aligned} Q(b, x, y) = {} & b^6 + (x+y)^4 b^4 + xy(x+y) b^3 \\ & + (xy(x+y)^3 + (x+1)^4 (y+1)^4 + x^2 y^2) b^2 \\ & + x^2 y^2 (x+y)(xy + x + y) b \\ & + x^2 (x+1)^2 y^2 (y+1)^2. \end{aligned}$$

Reducing Q modulo $b^2 = b + a$ we get

$$Q(b, x, y) = C(a, x, y) + D(a, x, y)b$$

with

$$\begin{aligned} C(a, x, y) &= a^3 + (x + y + 1)^4 a^2 \\ &\quad + xy(xy + x + y)\left(xy(x + y) + (x + 1)^2(y + 1)^2\right) a \\ &\quad + x^2(x + 1)^2 y^2 (y + 1)^2, \\ D(a, x, y) &= a^2 + xy(x + y)a + xy(x + 1)^2(y + 1)^2(xy + x + y). \end{aligned}$$

Summarizing we conclude for $x \neq y$ that $R_a(x) = R_a(y)$ implies $Q(b, x, y) = 0$ w.l.o.g., thus $a = b^2 + b$ for $b = C(a, x, y)/D(a, x, y)$. It remains to confirm that $D(a, x, y)$ has no zeros a in $\mathcal{T}_1$. On the contrary, suppose $D(a, x, y) = 0$. Then $C(a, x, y) = 0$ and $\mathrm{res}(C, D, a) = 0$. Here, we have

$$\mathrm{res}(C, D, a) = x^2(x + 1)^6 y^2 (y + 1)^6 (x + y)^2 (x + y + 1)^6.$$

Consequently $x + y + 1 = 0$, because $x, y \notin \mathrm{F}_2$ and $x \neq y$. On the other hand, from $C = D = 0$ we get a as a rational function in x and y, in our case

$$a = \frac{xy(x + 1)^2(y + 1)^2}{x^2 + xy + y^2 + 1}.$$

A substitution of $y = x+1$ yields $a = x^4+x^2$, which implies that $\mathrm{tr}(a) = 0$, a contradiction.

It remains to show that R_a does not attain the value 1. Conversely assuming $R_a(x) = 1$, i.e. $U_a(x) = V_a(x)$ we have to conclude that a has trace 0. To this end we apply the same technique as before and substitute $a = b^2+b$. Then the polynomial $U_a(x)+V_a(x)$ factorizes

$$U_a(x) + V_a(x) = Q(b, x)Q(b + 1, x)$$

with

$$Q(b, x) = b^4 + (x^4 + x + 1)b^2 + (x^3 + x^2)b + x^3 + x.$$

For C and D satisfying $Q = C + Db$ we compute

$$\begin{aligned} C(a, x) &= a^2 + (x^4 + x)a + x^3 + x, \\ D(a, x) &= x(x + 1)^3. \end{aligned}$$

Now $C = 0$ contradicts our assumption $x \notin \mathrm{F}_2$.

To confirm that S_a is one-to-one we compute in the same way as before for R_a:

$$\begin{aligned} Q(b, x, y) &= b^3 + (x + y)^2 b^2 + (x + 1)^2(y + 1)^2 b + xy(x + y + 1), \\ C(a, x, y) &= (x + y + 1)^2 a + xy(x + y + +1), \\ D(a, x, y) &= a + x^2 y^2, \\ \mathrm{res}(C, D, a) &= xy(x + y + 1)(x + 1)(y + 1). \end{aligned}$$

Thus $a = x^4 + x^2$, a contradiction.

To show that $S_a(x) \in \mathrm{F}_2$ is impossible the same method works. We leave the details to the reader. □

6. Proof of Theorem 1

Let $d_2 = (2^k - 1)\,3 + 1$, then obviously $\gcd(d_2, 2^n - 1) = \gcd(5, 2^k + 1)$ equals 5 for $k \equiv 2 \pmod 4$ and it equals 1 for $k \not\equiv 2 \pmod 4$. Thus, in both cases, there is an element b in F_{2^n} with $\alpha_2 b^{d_2} = 1$. Therefore

$$\|\alpha_2\|\|b^{d_2}\| = \|\alpha_2\|b^{d_1 d_2} = \|\alpha_2\|\|b\|^{d_2} = \|\alpha_2\|\|b\| = 1$$

and the substitution $x \leftarrow bx$ in $f(x)$ gives

$$f(bx) = \mathrm{tr}_L\left(\alpha_1\|bx\| + \alpha_2(bx)^{d_2}\right) = \mathrm{tr}_L\left(\frac{\alpha_1}{\|\alpha_2\|}\|x\| + x^{d_2}\right).$$

Now the general case $\alpha_1 + \overline{\alpha_1} = \|\alpha_2\|$ for Theorem 1 follows from $\alpha_2 = 1$ and $\alpha_1 + \overline{\alpha_1} = 1$.

Using Niho's theorem (Theorem 10) in order to confirm Theorem 1 we have to prove that, for all $c \in L = \mathrm{F}_{2^n}$, $n = 2k$, the number of $u \in \mathcal{S}$ such that

$$G_c(u) = u^5 + \overline{u}^5 + cu + \overline{cu} + 1 = 0$$

is either 0 or 2 (see (7)). Recall that

$$\mathcal{S} = \{u \in L : u\overline{u} = 1\},$$

$K = \mathrm{F}_{2^k}$, and $x \in K$ iff $x \in L$ and $x = \overline{x} = x^{2^k}$. We shall apply the approach described in Section 4. Recall that

$$\begin{aligned} &\beta = 1/(u + \overline{u}), \quad \mathrm{tr}(\beta) = 1,\\ &T = c + \overline{c},\\ &N = c\,\overline{c}. \end{aligned}$$

Case 1: $T = 0$, i.e. $c \in K$. Then $G_c(u) = 0$ iff

$$u^5 + \overline{u}^5 + c(u + \overline{u}) = 1,$$

i.e. iff

$$c = D_5(1/\beta)\beta + \beta = 1/\beta^4 + 1/\beta^2 + 1 + \beta,$$

where $D_5(X) = X^5 + X^3 + X$ denotes the 5th Dickson polynomial. Thus given c we have no or precisely two solutions $u \in \mathcal{S}$ of $G_c(u) = 0$ if and only if

$$\beta \mapsto \Phi(\beta) = 1/\beta^4 + 1/\beta^2 + \beta$$

is one-to-one for $\beta \in \mathcal{T}_1$, the set of elements in K with trace 1, which is true by Lemma 13. (For further details concerning this approach see [7, Section 4, Case 1] especially.)

Case 2a: $T = 1$. Note that this case occurs if and only if $u = 1$ is a solution of $G_c(u) = 0$. Then on the other hand $G_c(u)\,G_{\overline{c}}(u) = 0$ with $u \neq 1$ iff

$$c\overline{c} = \Psi(\beta) = 1/\beta^8 + 1/\beta^2 + \beta, \tag{12}$$

where $\beta = 1/(u + \overline{u}) \in K$ and therefore $\mathrm{tr}_K(\beta) = 1$, see (10). Arguing as before in Case 1 we have to show that Ψ is one-to-one on $\mathcal{T}_1$, which is true by Lemma 13. The two solutions

of $G_c(u) = 0$ and $G_{\overline{c}}(u) = 0$ are $u = 1$ and $u = u_0$, respectively $u = 1$ and $u = \overline{u_0}$, where $\beta_0 = 1/(u_0 + \overline{u}_0)$ is the unique solution of (12) with trace 1.

Case 2b: $T \notin \mathrm{F}_2$. By (10), we have

$$N = T^2\beta^2 + \Phi_1(\beta)\, T + \Phi_1(\beta)^2$$

with

$$\Phi_1(\beta) := (D_5(1/\beta) + 1)\, \beta = \Phi(\beta) + 1.$$

We have to show that for each $T \notin \mathrm{F}_2$

$$\beta \mapsto T^2\beta^2 + \Phi_1(\beta)\, T + \Phi_1(\beta)^2$$

maps two-to-one for $\beta \in \mathcal{T}_1$. (For details concerning this approach we refer again to [7, Section 4, Case 2] in particular.) In other words, since $u = 1$ is impossible (see Case 2a above), given $T \notin \mathrm{F}_2$ and β with $\mathrm{tr}_K(\beta) = 1$, we have to show that there is a unique non-zero Δ with $\mathrm{tr}_K(\Delta) = 0$ and

$$T^2\beta^2 + \Phi_1(\beta)\, T + \Phi_1(\beta)^2 = T^2(\beta + \Delta)^2 + \Phi_1(\beta + \Delta)\, T + \Phi_1(\beta + \Delta)^2, \tag{13}$$

that is

$$\Delta^2 = (\Phi_1(\beta + \Delta) + \Phi_1(\beta))\,/\,T + (\Phi_1(\beta + \Delta) + \Phi_1(\beta))^2\,/\,T^2.$$

Setting $\Delta = x^2 + x$, this means that

$$x^2 + \Big(\Phi_1(\beta + x^2 + x) + \Phi_1(\beta)\Big)\,/\,T + \varepsilon = 0$$

or equivalently

$$T = \frac{\Phi_1(\beta + x^2 + x) + \Phi_1(\beta)}{x^2 + \varepsilon} \tag{14}$$

for an unique set $\{x, x + 1\}$ and $\varepsilon \in \mathrm{F}_2$. The pairs (x, ε) and $(x + 1, \varepsilon + 1)$ give the same T. Hence w.l.o.g. we can choose $\varepsilon = 0$. Then the right-hand rational function of Eq. (14) coincides with $R_a(x)$ for $a = \beta^2$, since $\Phi_1(\beta) = \Phi(\beta) + 1$, see (11). Thus the existence of an unique non-zero $\Delta = x^2 + x$ for given T and β is guaranteed in view of Lemma 14. This completes the proof that the Boolean function f in Theorem 1 is bent. □

7. Proof of Theorem 2

Let k be odd. We can w.l.o.g. assume that $\alpha_1 + \overline{\alpha_1} = 1$ and $\alpha_2 = 1$, because d_2 is invertible. (In fact $s_2 = \frac{1}{4}$ and therefore $2s_2 - 1 = -\frac{1}{2}$, which is invertible modulo $2^k + 1$; see Section 4.) Since $s_1 = \frac{1}{2}$ and $s_2 = \frac{1}{4}$, according to (the general form of) Niho's theorem, we have to show that

$$G_c(u) = cu^2 + \overline{cu}^2 + u + \overline{u} + 1$$

has either 0 or 2 zeros u in $\mathcal{S}$. The case $c \in K$ is trivial. If $c \notin K$ we consider

$$G_c(u)\, G_{\overline{c}}(u) = 0$$

and substitute as before β, T and N with the condition $\mathrm{tr}_K(\beta) = 1$. This leads to the following equation in K:

$$(T^2+1)\beta^4 + (T+1)\beta^2 + T\beta + N = 0, \tag{15}$$

which is linear in β. If $T = 1$ then $N = \beta$, i.e. we have a unique solution as desired in this special case, where $G_c(1) = 0$ (see Case 2a above).

Thus assume $T \notin \mathrm{F}_2$ in the sequel (see Case 2b in the preceding proof). We have to verify that the homogeneous equation corresponding to (15) has exactly one non-zero root Δ with trace 0:

$$(T^2+1)\Delta^3 + (T+1)\Delta + T = 0. \tag{16}$$

After the substitution $\Delta = a^2 + a$ the left hand term factorizes $Q(a)\, Q(a+1)$ with

$$Q(a) = a^3 T + a^3 + 1.$$

W.l.o.g. assume $Q(a) = 0$. Since k is odd, we know that 3 is invertible modulo $2^k - 1$. Consequently

$$\Delta = (T+1)^{-\frac{2}{3}} + (T+1)^{-\frac{1}{3}}$$

and vice versa this is a solution of (16). (Actually we can also conclude that *every* solution Δ has trace zero.) Therefore if (15) has a solution at all, then it has precisely 2 solutions with the same trace. This completes the proof. □

8. Proof of Theorem 3

Let k be even. Hence $\frac{1}{3} \pmod{2^k+1}$ exists. Again w.l.o.g. we can assume that $\alpha_1 + \overline{\alpha_1} = 1$ and $\alpha_2 = 1$, because d_2 is invertible. (In fact $s_2 = \frac{1}{6}$ and therefore $2s_2 - 1 = -\frac{2}{3}$, which is invertible modulo $2^k + 1$; see Section 4.)

Since $s_1 = \frac{1}{2}$ and $s_2 = \frac{1}{6}$, by Niho's theorem, we have $G_c(u) = cu + \overline{cu} + u^{\frac{2}{3}} + \overline{u}^{\frac{2}{3}} + 1$. Taking third powers is one-to-one on $\mathcal{S}$. Thus $G_c(u)$ can be replaced by

$$G_c(u) = cu^3 + \overline{cu}^3 + u^2 + \overline{u}^2 + 1.$$

In what follows parameters γ, β, T and N are used, which are defined as before.

Case 1: $c \in K$. Then $G_c(u) = 0$ is equivalent to

$$(c+\beta)\left(\beta^2 + 1\right) = 0$$

Note that $\beta \neq 1$, since $\mathrm{tr}_k(\beta) = 1$, but $\mathrm{tr}_K(1) = 0$ (k is even). Hence $c = \beta$, and we have at most one solution as desired.

Case 2: $c \notin K$. We consider $G_c(u)\,G_{\overline{c}}(u) = 0$, which becomes after substitution the following equation in K:

$$\gamma^4 + 1 + (\gamma^2 + 1)D_3(\gamma)T + D_3(\gamma)^2 N + T^2 = 0, \tag{17}$$

where $D_3(X) = X^3 + X$ denotes the 3rd Dickson polynomial. (This is of course also included in the general formula (10). Using the iteration rule $D_i(D_j(X)) = D_{ij}(X)$ for Dickson polynomials, here with $i = 3$ and $j = \frac{2}{3}$, it follows if β is replaced by $1/D_3(\gamma)$.) In term of β we get

$$F_T(\beta) := \beta^2 + T\beta + \frac{\beta^6}{\beta^4 + 1}T^2 = N. \tag{18}$$

Case 2a: $c + \overline{c} = 1$. If $T = 1$ then the preceding equation becomes

$$F_1(\beta) = \beta + \frac{\beta^2}{\beta^4 + 1} = N.$$

We have to show that F_1 is one-to-one on $\mathcal{T}_1$, the set of all elements in K with trace 1. This is in fact a consequence of Lemma 13, since $\mathrm{tr}_K(1) = 0$ and

$$F_1(\beta + 1) = 1/\beta^4 + 1/\beta^2 + \beta + 1 = \Phi(\beta) + 1.$$

Case 2b: $T \notin \mathrm{F}_2$. We have to show that for each β and T, there is precisely one non-zero Δ with trace 0, such that $F_T(\beta) + F_T(\beta + \Delta) = 0$. We argue as in the proof of Theorem 1 in Case 2b. In the present case, we can reduce the latter statement to the fact that S_a in Lemma 14 induces a permutation of $K \setminus \mathrm{F}_2$. This completes the proof of Theorem 3. □

References

[1] M. Daum, H. Dobbertin, G. Leander, An algorithm for checking normality of Boolean functions, in: Proceedings of the Workshop on Coding and Cryptography (WCC 2003), Versailles, France, March 2003, pp. 133–142.

[2] J.F. Dillon, Elementary Hadamard difference sets, in: Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, Florida, Congressus Numerantium No. XIV, Utilitas Mathematics, Winnipeg, Manitoba, 1975, pp. 237–249.

[3] J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. 10 (2004) 342–389.

[4] H. Dobbertin, Construction of bent functions and highly nonlinear balanced Boolean functions, in: B. Preneel (Ed.), Fast Software Encryption, Lecture Notes on Computer Science, vol. 1008, Springer, Berlin, 1995, pp. 61–74.

[5] H. Dobbertin, One-to-one highly nonlinear power functions on GF(2^n), AAECC Applicable Algebra in Engineering, Comm. Comput. 9 (1998) 139–152.

[6] H. Dobbertin, Uniformly representable permutation polynomials, in: T. Helleseth, P.V. Kumar, K. Yang (Eds.), The Proceedings of "Sequences and Their Applications–SETA '01", Springer, London, 2002, pp. 1–22.

[7] H. Dobbertin, P. Felke, T. Helleseth, P. Rosendahl, Niho type cross-correlation functions via Dickson 33 polynomials and Kloosterman sums, IEEE Trans. Inform. Theory, to be published.

[8] R.L. McFarland, A family of difference sets in non-cyclic groups, J. Combin. Theory Ser. A 15 (1973) 1–10.

[9] Y. Niho, Multivalued cross-correlation functions between two maximal linear recursive sequences, Ph.D. Thesis, University of Southern California, 1972.
[10] K. Nyberg, Perfect non-linear S-boxes, in: D.W. Davies (Ed.), Advances in Cryptology—Eurocrypt '91, vol. 547, Lecture Notes in Computer Science, Springer, Berlin, 1991, pp. 378–386.
[11] O.S. Rothaus, On "bent" functions, J. Combin. Theory Ser. A 20 (1976) 300–305.